National Aeronautics and Space Administration

Leveraging Commercially Issued Multi-Factor Identification Credentials

Tim W. Baldridge
Office of the Chief Information Officer
George C. Marshall Space Flight Center

Agenda

- Introduction
- ICAM Overview
- Identity vs. Credential Life Cycle Management
- Trust Ecosystem
- PIV and PIV-I Cards
- Multi-Factor Tokens
- Derived Credentials
- @ NASA
- Lessons Learned

Some NASA details

- NASA includes:
  - » 20,000 civil servant employees
  - » 55,000 on-site and near-site contractors
  - » At least 25,000 Additional partners world-wide
- NASA's system/application landscape includes:
  - » 3,000 applications, most built in-house
  - » Mission control, research labs, product fabrication, more
  - » Every flavor of every operating system, hardware, software….
- Historically, NASA has been:
  - » Highly decentralized
  - » Autonomous Centers with a B-to-B network infrastructure
  - » Characterized by weak CIO governance
- HSPD-12 helped us:
  - » Implement a robust Identity, Credential, and Access Management Architecture

I can...
with ICAM
Identity, Credential, and Access Management

ICAM Overview @ NASA

Identity Management and Account eXchange (IdMAX) – Single Authoritative source of all NASA identities

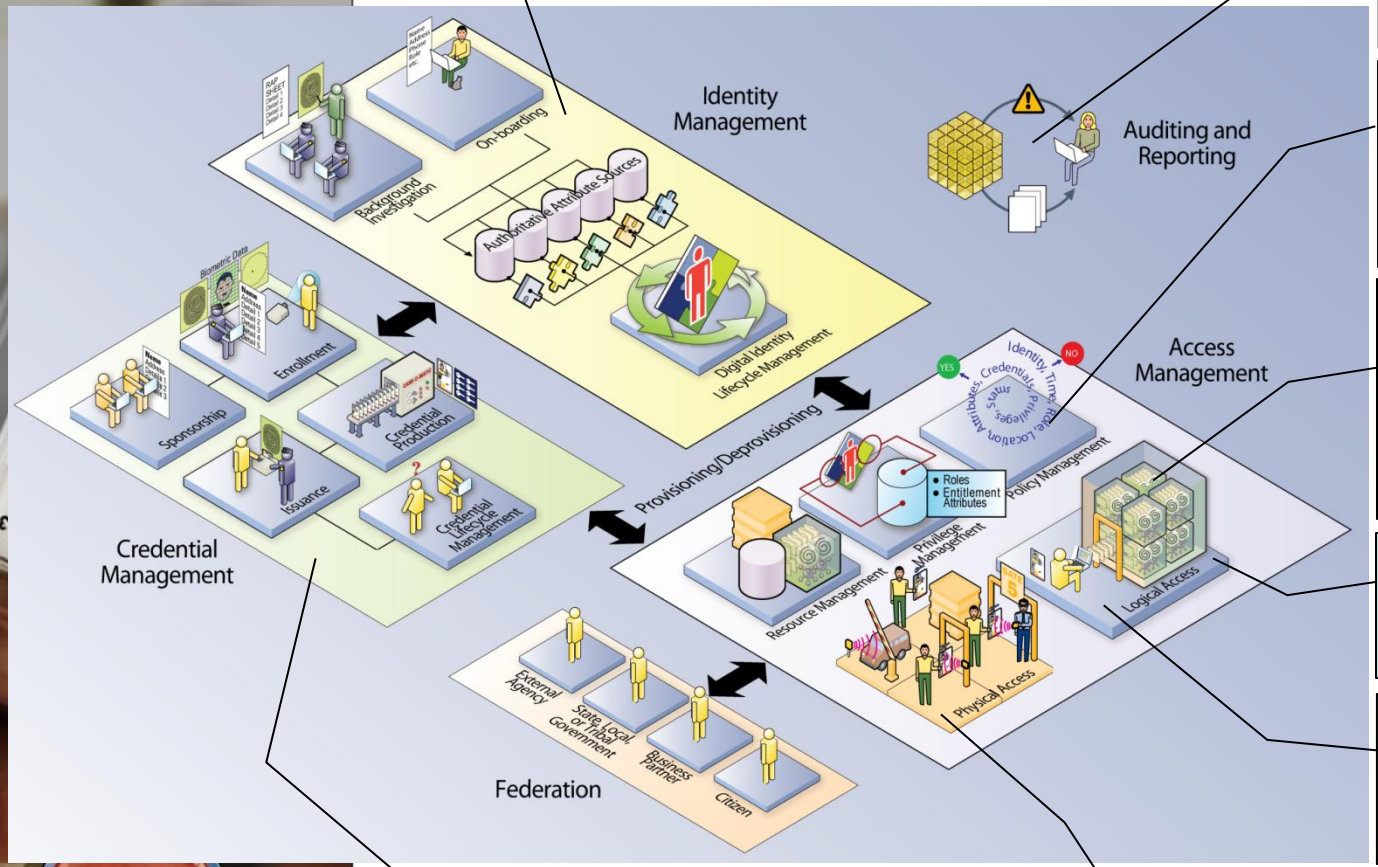
ICAM Audit Viewer allows us to track every change made to a person.

IdMAX manages account request and approval for NASA applications, and automatically provisions to the Launchpad.

NASA's Consolidated Active Directory (NCAD) controls access to desktops and applications such as e-mail and SharePoint.

The Access Launchpad provides access control for web-based applications.

The Agency RSA infrastructure supports applications that cannot use PIV smartcards.



IdMAX manages issuance of PIV credentials, RSA Tokens, AD accounts, and Launchpad Accounts.

The Enterprise Physical Access Control System (EPACS) controls access to buildings and doors throughout NASA.

Identity vs. Credential Life Cycle Management

- A Credential Is Not an Identity – It Is Used To Assert A Represented Identity
- An Individual May Have Multiple Credentials
- Identity and Credential Life Cycle Events May Be But Are Not Necessarily Coincident
  - » Replaced Credential vs. Relationship Change
- Effective Identity Management Critical to Fair Information Practice Principles

Credential Identifiers

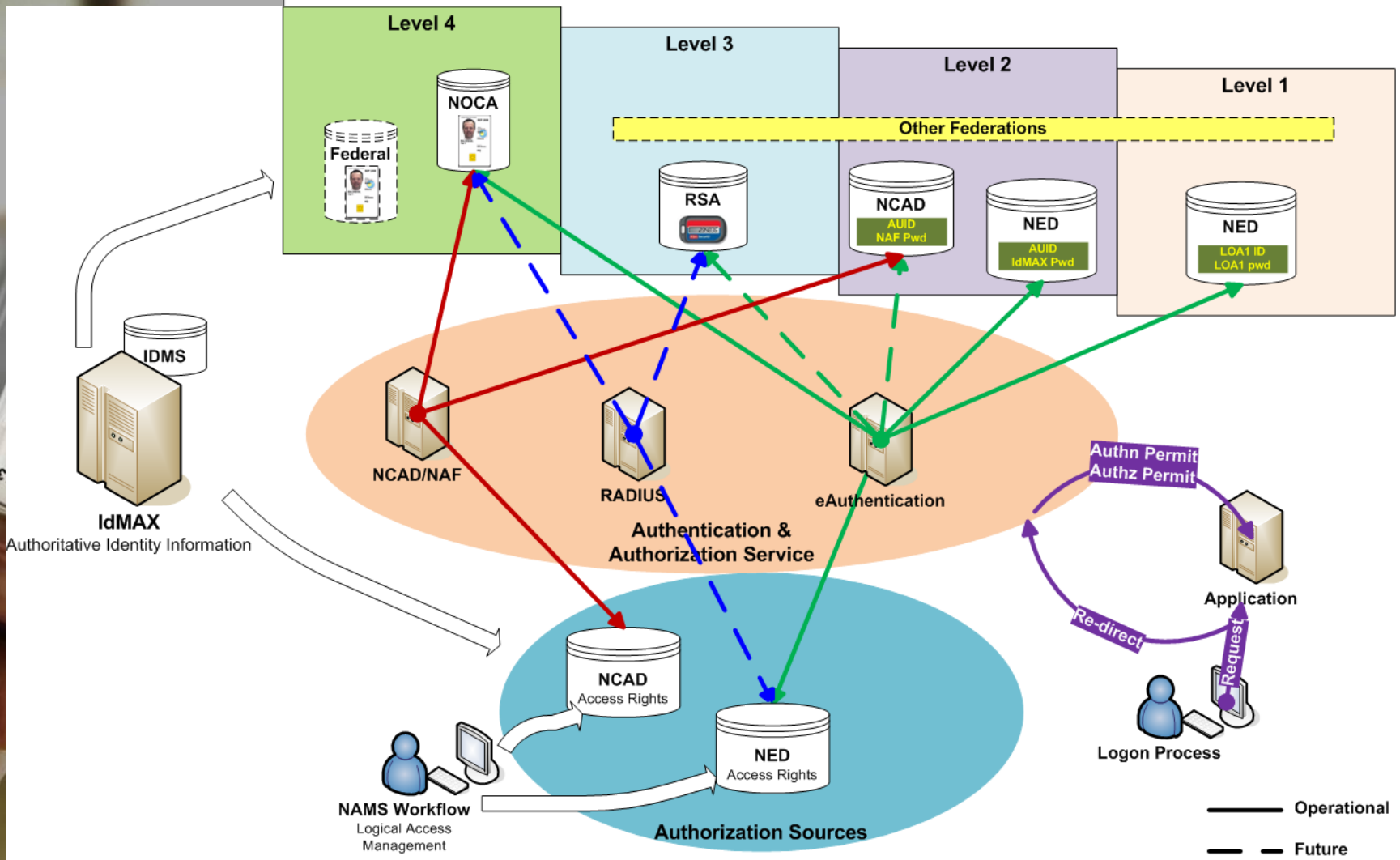
- PIV – FASC-N
  - » Federal Agency Smart Credential Number
    - Defined and assigned by U.S. Federal Agencies
  - » Place holder for GUID
- PIV-I – GUID/UUID
  - » FASC-N May Not Be Used
  - » GUID is defined by RFC 4122
- Parallel Person IDentifier – PPID
  - » Pair Wise IDPs Cross-Link Person IDs
  - » RFC 4122 Ideal for Person IDs

Logical Access Management PIV Enablement Strategy

- Provide Central Authentication and Authorization (A&A) Service
  - » PIV-enable the A&A service
  - » Applications integrate with the A&A service, not directly to PIV
- A&A Service supports credentials at all levels of assurance
  - » Applications can use mixed sets of credentials according to system needs and users' capabilities
  - » Users get Single Sign-on benefit

I can...
with ICAM
Identity, Credential, and Access Management

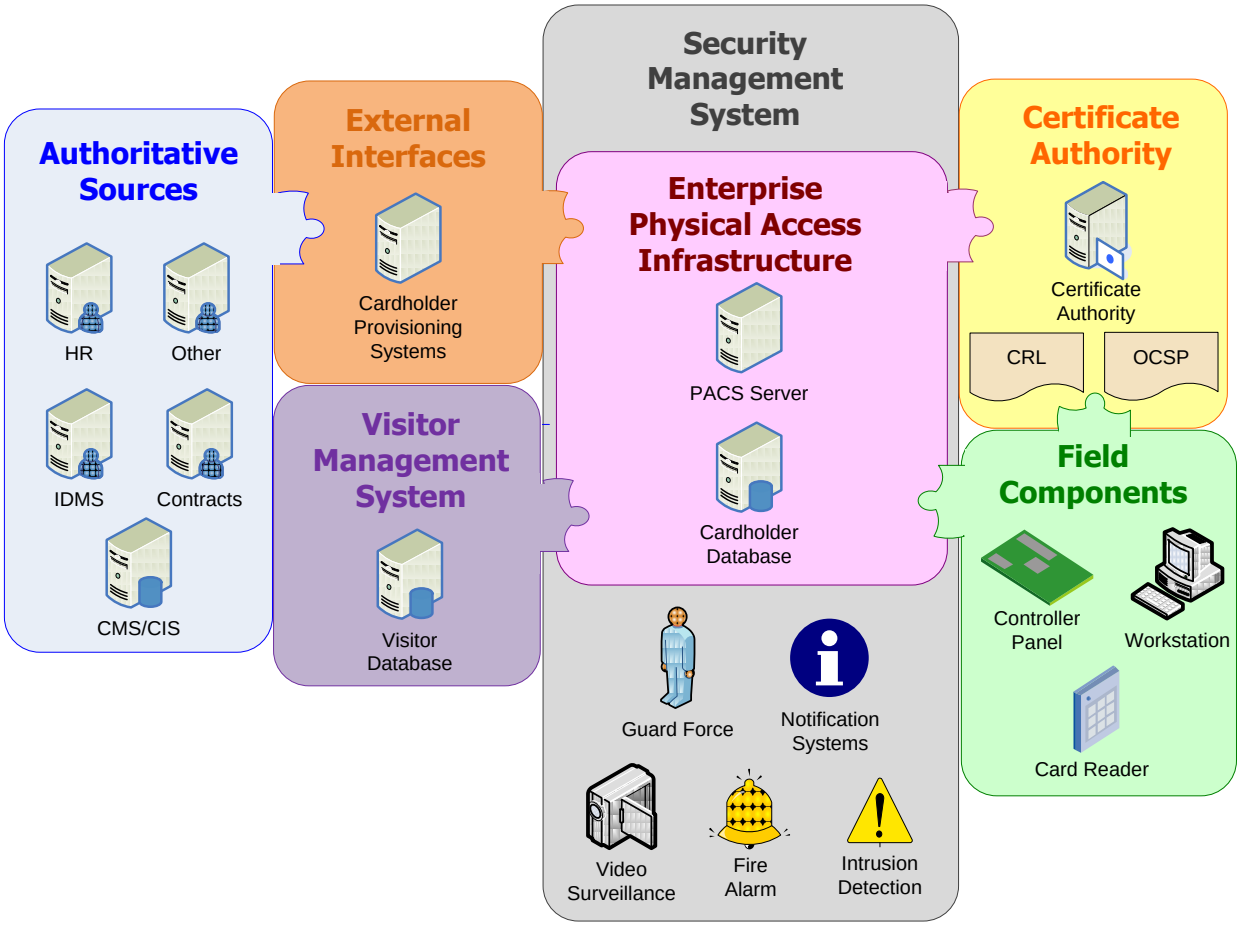
Authentication & Authorization Service Description



Physical Access Management PIV Enablement Strategy

- Enterprise Physical Access Control System (EPACS) Operational At NASA Since 2005
  - » All NASA Centers Use A Common EPACS System Provisioned From IdMAX
  - » Building/Door Readers Have Been Converted To Read PIV Smartcards

PACS Architecture



Trust Ecosystem

- Draft National Strategy for Trusted Identities in Cyberspace – NSTIC
  - » http://www.dhs.gov/xlibrary/assets/ns_tic.pdf
- Trusted Framework Adoption Process For Levels of Assurance 1, 2, and non-PKI 3
  - » http://www.idmanagement.gov/documents/TrustFrameworkProviderAdoptionProcess.pdf
- Identity Scheme Adoption Process
  - » http://www.idmanagement.gov/documents/IdentitySchemeAdoptionProcess.pdf
- Open Identity Solutions for Open Government
  - » http://www.idmanagement.gov/drilldown.cfm?action=openID_openGOV

PKI Trust Governance For Non-Federal Issuers (NFIs)

- The Federal Bridge Certification Authority (FBCA) Certifies NFIs For Use By Federal Relying Parties For LOA 3 (PKI) and LOA 4
- The FBCA Certificate Policy (CP) Contains The Detailed Requirements That Those NFIs Must Meet
- There Is No Intent Or Expectation For Trust By U.S. Federal Departments And Agencies Of Cards Or Tokens Where Certificates Are Issued Outside The Federal PKI Policy Authority

PKI in the Trust Ecosystem

- Emerging Threats to Online Trust: The Role of Public Policy and Browser Certificates
- Use of PKI for PIV and PIV-I
- Use of PKI for exchanging Federation Metadata
- Use of PKI by Commercial SSPs for PKI Tokens
- Trust anchors – largely unmanaged by RPs

PIV Cards

- Personal Identification Verification Cards
  - » Cornerstone Electronic Credential In U.S. Federal Government Used In Authentication To Both Information Resources And Facilities
  - » In HSPD-12 U.S. Federal Departments And Agencies Are Required To Issue PIV Cards to Permanent Government Personal And Contractors
  - » Issued ONLY By U.S. Federal Entities
  - » Is Relied On By U.S. Federal And Non-Federal Entities
  - » Background Investigation – Minimum NACI
  - » Assert Federal Common Policy Framework (FCPF) Certificate Policy OIDs for PIV

PIV-I … PIV Interoperable Cards

- Personal Identification Verification – Interoperable (by Non-Federal Issuers – NFI) Cards
  - » Cornerstone Credential For All Security Controls For Both Information Resources And Facilities Protection
  - » Intended Primarily For Issuance By Non-Federal Entities
  - » May Be Relied On By Federal And Non-federal Entities
  - » Identity and Affiliation Certainty Equivalent to PIV
  - » No Issuer Background Investigation of Cardholders
  - » Asserts Federal Bridge Certificate Authority (FBCA) Certificate Policy OIDs for PIV-I

Multi-Factor Tokens
Alternate Form Factor - PIV

- Facility Access Cards – may be equivalent card issuance and technical interoperability to PIV-I where local policy states a deliberate position against interoperability through the trust ecosystem
- Non-card form factor smartcard technology
- Micro-SD which is electronically equivalent to PIV combined with PDA using NFC (Near field Communication) for both LACS and PACS
- Trusted by U.S. Federal If Certificates Issued Under FBCA Certificate Policy – MediumHW

Derived Credentials

- The Binding Of A Secondary Credential At End-user Activation To An Identity Based On Verification Of A Direct Issued Credential
- Why Is This Important?
- It Will Allow Strong Identity Binding For Alternate Form Factor And Pseudonym Credentials For A Myriad Of Purposes
- The Binding Of A Derived Secondary Credential May Be At The Same Or Lower Level Of Assurance

What We Do Today @ NASA

- Smartcard Login To The Desktop With Access To Over 565 Applications Without Additional Logon Prompts
- Any NASA Worker Can Visit Any NASA Center:
  - » Pre-authorized Access To Any Building/Room
  - » Wireless Access To The NASA Network
- Ensure On A Person-by-person Basis That Those Who Need IT Security Training Have Taken It
- Provide “Basic Level Of Entitlement” Access To IT Systems Based On Identity Attributes
- Initiate “Close Account” Processes On 91% Of Our IT Assets When Someone Leaves

Cool Stuff We're Planning

- Establish A Non-PIV Smartcard (Multi-factor Token) For Use By Temporary Workers And Others
  - » Allows Us To Lock IT Systems Down To Smartcard-only
- Assign A Level Of Risk To Each Access Role In Our IT Systems
  - » Automatic Comparison Of Level Of Risk Of The Asset To Level Of Confidence In A Person
  - » Allows Early Access To Low-risk Systems, While Protecting Our Higher-risk Systems
- Link Training Requirements To Each Access Role
  - » Automatic Check Against Our Training System To Ensure Proper Training For The Role Has Been Completed

What Does This All Mean?

- It Means Relying Parties (RPs) Are In Control
- RPs Decide If
  - » Assurance Levels Provide Sufficient Granularity
  - » Certificate Policies Provide Sufficient Granularity
  - » Issuer (Name) Constraints Are Required
  - » To Accept Alternate Form Factors (HW & SW)
- There Are Ample Controls In The Trust Framework For RPs To Admit Only Authorized Accesses
- Bottom Line – A Card Or Token With Certificates Assert A Certificate Policy That The RP Can Map To Access Privileges

Lessons Learned

- Look at PIV enablement in the context of a robust ICAM architecture
  - » Access Management doesn't work if Identity and Credential Management aren't working
  - » PIV enablement doesn't work for people who don't have PIV smartcards
  - » …or can't use them
- Implement a "killer app" to jumpstart adoption
- Scorecards seem mean…but they tend to work
- Communications, communications, communications!
  - » Most people don't get ICAM
  - » Sell Security on how fast you can get bad guys out
  - » Sell the application owner on ease of account management
  - » Sell the user on Single Sign On

National Aeronautics and Space Administration

How can you increase your ICAM value?

Tim.Baldridge@nasa.gov

National Aeronautics and Space Administration

BACK-UP SLIDES

Fair Information Practice Principles (FIPPs)

- http://www.ftc.gov/reports/privacy3/fairinfo.shtm
- http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf
- Eight core principles of privacy protection:
  1. Transparency
  2. Individual Participation
  3. Purpose Specification
  4. Data Minimization
  5. Use Limitation
  6. Data Quality and Integrity
  7. Security
  8. Accountability and Auditing

Normative PIV-I Reference Documents

- http://www.idmanagement.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf
- http://www.idmanagement.gov/fpkipa/documents/pivi_certificate_crl_profile.pdf
- http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers.pdf
- http://www.idmanagement.gov/documents/PIV-I_FAQ.pdf
- http://csrc.nist.gov/publications/drafts/800-63-rev1/SP800-63-Rev1_Dec2008.pdf

FBCA Supplementary Antecedent, In-Person Definition

- An Antecedent event is an in-person proofing event that occurred previously and may suffice as meeting the in-person identity proofing requirements.

- http://www.idmanagement.gov/fpkipa/documents/FBCA_Supplementary_Antecedent.pdf

FBCA CP 3.2.3.1 Authentication of Human Subscribers (Medium Assurance)

- Identity shall be established by in-person proofing before the Registration Authority, Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided shall be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement. Credentials required are one Federal Government-issued Picture I.D., one REAL ID Act compliant picture ID, or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Non-REAL ID Act compliant Drivers License). Any credentials presented must be unexpired.
- Clarification on the trust relationship between the Trusted Agent and the applicant, which is based on an in-person antecedent identity proofing event, can be found in the *"FBCA Supplementary Antecedent, In-Person Definition" document.*
- **For PIV-I, credentials required are two identity source documents in original form. The identity source documents must come from the list of acceptable documents included in *Form I-9, OMB No. 1115-0136, Employment Eligibility Verification. At least one document shall be a valid State or Federal Government-issued picture identification (ID).***
  For PIV-I, the use of an in-person antecedent is not applicable.